

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
20 March 2003 (20.03.2003)

PCT

(10) International Publication Number  
WO 03/024020 A1

(51) International Patent Classification<sup>7</sup>: H04L 9/32,  
9/18, 9/18, G06K 9/64

(21) International Application Number: PCT/US01/29031

(22) International Filing Date:  
10 September 2001 (10.09.2001)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US): **ENTRIQ LIMITED BVI** [GB/GB]; Abbot Building, P.O. Box 3186, Road Town, Tortola (VG).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **MCLEAN, Ivan** [ZA/US]; 5541 Fermi Court, Ste. 220, Carlsbad, CA 92008 (US).

(74) Agents: **MALLIE, Michael, J.** et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th Floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

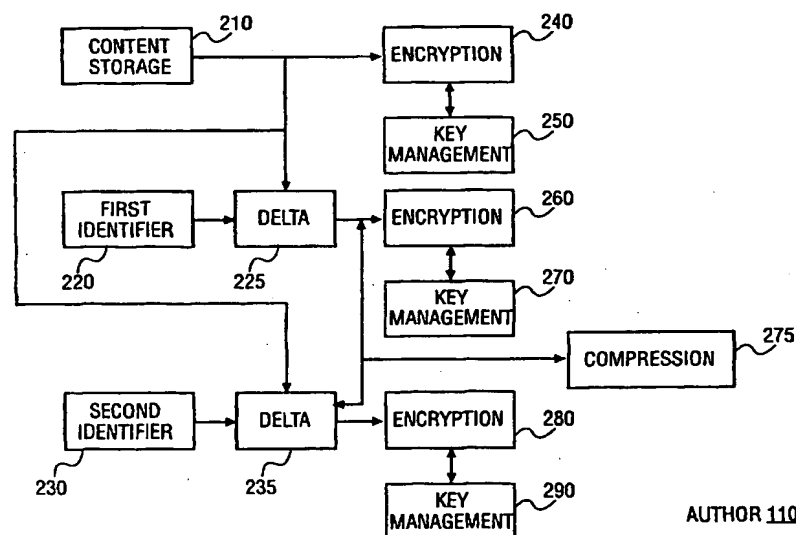
(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND COMPUTER SYSTEM TO PERFORM ON THE FLY FINGERPRINTING FOR MEDIA CONTENT



(57) Abstract: A method and system to perform on the fly fingerprinting for media content (210) is disclosed. An author server (110) transmits (275) a content stream (210) such as a video clip to a client. The content stream (210) includes a series of content frames. The author server (110) also transmits a watermark (225, 235) for every content frame to the client. One watermark (225) is generated from a first identifier (220); the other (235), from a second identifier (230). The author server (110) generates a sequence of watermarks (225, 235) in a manner that is unique for a particular client. The unique sequence constitutes the fingerprint for the client. The client inserts every watermark (225, 235) from the sequence into its associated content frame.

## METHOD AND COMPUTER SYSTEM TO PERFORM ON THE FLY FINGERPRINTING FOR MEDIA CONTENT

### FIELD OF INVENTION

[0001] The present invention relates generally to the fields of data processing and fingerprinting. Specifically, the present invention relates to a method and a computer system to perform on the fly fingerprinting for media content.

### BACKGROUND OF THE INVENTION

[0002] Fingerprinting is the process of inserting an identifier in text, audio and video content. The identifier can uniquely identify the source (server) of the content or the recipient (client) of the content. Fingerprinting can prevent illegal copying and distribution of the content.

[0003] A good application for fingerprinting is in the area of multicasting. Multicasting is the process in which a single server transports content to multiple clients at the same time. Illegal copying and distribution of the transported content during multicasting is a disturbing worldwide problem. For example, copies of video content, e.g., Hollywood blockbusters, are routinely made using devices such as the videocassette recorder (VCR) and pirated to foreign countries. This results in an enormous loss of revenues to the companies that hold the licensing rights to the multicast content.

[0004] Fingerprinting is an expensive process because of the high central processing unit (CPU) time that is required to compute every fingerprint. In the prior art, both the server (e.g. media server) and the client can perform fingerprinting. The prior art has several shortcomings. Fingerprinting at the media server end can increase the workload of the already busy server. The processing overhead can introduce a bottleneck and the media server can become paralyzed during the spikes in demand, (e.g. when transporting a live sports event). Fingerprinting at the client end is not desirable for at least two

reasons. One, clients such as the set top box (STB), personal digital assistant (PDA) and cell phone may not be able to provide the processing power necessary to do the fingerprint computation and insertion. Even the high-powered personal computers (PC) may have severe limitations in allocating resources to compute and insert a robust fingerprint. Two, a hacker can disable the client fingerprinting module.

### **SUMMARY OF THE INVENTION**

[0005] For one aspect of the present invention, a computer-implemented method to fingerprint content including a plurality of content frames is disclosed. A sequence of identifiers is generated by associating either a first or a second identifier with each content frame of at least a portion of the plurality of content frames. The plurality of content frames and the sequence of identifiers are transmitted to a client. Each identifier of the sequence of identifiers is inserted into an associated content frame of the plurality of content frames at the client. The sequence of identifiers is generated in a manner that it is unique for the client.

[0006] For another aspect of the present invention, a computer-implemented method to fingerprint a content frame is disclosed. The content frame is corrupted by removing a noise signal from the content frame. A watermark delta is computed by adding an identifier to the noise signal. The corrupt content frame and the watermark delta are transmitted to a client. The watermark delta is inserted into the corrupt content frame by the client.

### **BRIEF DESCRIPTION OF THE DRAWINGS**

[0007] The present invention is illustrated by way of example and not limitation in the figures of the accompanying drawings, in which like references indicate similar elements, and in which:

[0008] **Figure 1** illustrates an exemplary embodiment of the media network to perform on the fly fingerprinting for media content;

[0009] **Figure 2** illustrates one embodiment of the author module;

- [0010] Figure 3 illustrates an alternate embodiment of the author module;
- [0011] Figure 4 illustrates an exemplary embodiment of the media server;
- [0012] Figure 5 illustrated an exemplary embodiment of the client machine;
- [0013] Figure 6 illustrates exemplary embodiments of the data streams to perform client side fingerprinting (or watermarking) for multicast data;
- [0014] Figure 7 illustrates one embodiment of a method to perform on the fly fingerprinting for media content;
- [0015] Figures 8A and 8B illustrate an alternate embodiment of the method to perform on the fly fingerprinting for media content; and
- [0016] Figure 9 illustrates a computer in block diagram form, which may be representative of any author module, media server or client machine.

#### **DETAILED DESCRIPTION**

[0017] A method and a computer system to perform on the fly fingerprinting for media content are described. A media network is described including an author module, a media server, and a client machine. For one aspect of the present invention, the author module transmits an encrypted content frame, an encrypted first identifier and an encrypted second identifier to the media server. The content can be audio, video, or data content. The content frame can be an audio, video or data frame. The first and second identifiers can be watermarks. In this description, the terms transmit and transport are used interchangeably.

[0018] The content and the first and second identifiers can be transmitted as three different data streams. It will be appreciated that several technologies and methods exist to transmit the content and the identifiers. For example, for the author module, media server and client machine that are moving pictures expert group (MPEG) standard 4 (MPEG-4) compatible, the content can be streamed through the base layer, and the first and second identifiers can be streamed through the first and second enhancement layers, respectively. For another example, for the author module, media server and

client machine that are MPEG standard 2 (MPEG-2) compatible, the content and the identifiers can be streamed as Intellectual Property Management & Protection (IPMP) message streams, key streams, protection streams or a combination thereof. It will be appreciated that the method and computer system of the present invention are applicable to any open standard such as MPEG-2 or QuickTime™.

[0019] The media server selects either the first or the second identifier to associate with the content frame. The media server acts as a switch in selecting between the first and second identifiers for every content frame that is transmitted to the client. The media server thus generates a sequence of identifiers for the particular client. The media server can select the series of identifiers in a manner such that the sequence is unique to the particular client. The following example illustrates the point.

[0020] Suppose the media server is requested to transmit a video clip. For the purposes of illustration, we consider five image frames of this video clip. Suppose the media server is requested to transport the video clip to three different clients. For the first client, the media server can select the sequence of identifiers to include the first, first, second, first and second (11212) identifiers to be associated with frames one through five, respectively. For the second client, the media server can select the sequence of identifiers to include the second, first, second, second and second (21222) identifiers to be associated with the frames one through five, respectively. For the third client, the media server can select the sequence of identifiers to include the second, second, first, second and first (22121) identifiers to be associated with the frames one through five, respectively. The media server can thus generate a unique sequence of identifiers for every one of the three clients. It will be appreciated that for a Hollywood blockbuster that includes countless image and audio frames, the media server can generate unique sequences of identifiers for thousands or even millions of different clients. It will be appreciated that embodiments in which the media server generates the sequences only for a portion of the content frames of the content are possible.

For example, the media server can generate the sequences for the first one hundred content frames that are multicast. For another example, the media server can generate the sequences by associating the identifiers with every alternate content frame of the content instead of every content frame that is transported. It will be appreciated that for real word presentations with a high number of frames, the unique sequence can be repeated ad infinitum for a particular client. For example, if the video clip mentioned above has more than five frames, the sequence 11212 can be repeated ad infinitum for the first client.

[0021] The media server transmits the selected identifier and the content frame to the client machine. The client machine decrypts the selected identifier and content frame and inserts the selected identifier into the content frame. The client machine can perform the decryption operation in real time or at a later time by storing the encrypted identifier and content frame. The processing overhead for the client machine is extremely low because the client machine effectively performs an exclusive OR (XOR) operation to insert the selected identifier into the content frame. The fingerprinting technique described above can be referred to as being performed on the fly.

[0022] A concern regarding client side fingerprinting is that it allows the hacker to intercept the content before the fingerprinting operation takes place. The hacker can also disable the fingerprinting capabilities of the client machine altogether. The second aspect of the present invention addresses this concern.

[0023] According to another aspect of the present invention (also referred to as the second aspect) the author module removes a noise signal from a content frame such that the content frame is corrupted. The noise signal can be a low bandwidth random noise signal. The author module selects the noise signal such that the commercial value of the corrupt content frame is effectively destroyed. The author module can also select the noise signal such that the amount of data that is removed from the content frame is small. The author module adds the noise signal to a first identifier and to a second

identifier. As stated previously, the first and second identifiers can be watermarks. The resultant signal of the addition of the noise signal and first identifier is referred to as the first watermark delta.

[0024] In this description, the term watermark delta is defined to include a watermark, the delta between an original content frame and a watermarked content frame, or the resultant signal of the addition of the noise signal and an identifier. Also, in this description, wherever appropriate, the term content is defined to include both original uncorrupt content and corrupt content to avoid undue repetition and complexity.

[0025] The resultant of the addition of the noise signal and the second identifier is referred to as the second watermark delta. The author module encrypts the corrupt content frame and the first and second watermark deltas. The author module transmits the encrypted corrupt content frame and the first and second watermark deltas to the media server. The media server selects either the first watermark delta or the second watermark delta to associate with the corrupt content frame. The media server transmits the corrupt content frame and the selected watermark delta to the client. The client machine decrypts the corrupt content frame and the selected watermark delta and inserts the selected watermark delta into the corrupt content frame.

[0026] The second aspect of the present invention provides robust security from the hacker because the content frame itself is worthless without the insertion of the selected watermark delta. The second aspect of the present invention can significantly lower the bandwidth requirement to perform client side fingerprinting because the removal of the noise signal from the content frame reduces the content frame size. Also, the noise signal and the watermarks can be selected intelligently such that they are very good candidates for data compression.

[0027] Figure 1 illustrates an exemplary embodiment of the media network 100 to perform on the fly fingerprinting for media content. The media network 100 is shown including the author module 110, the media server 120 and the client machine 130. The media server 120 interfaces to the

author module 110 and the client machine 130. Each of these modules can be a separate processing device or hardware and/or software modules operating within the media network 100 to process instructions or code for performing the operations described herein.

[0028] In one embodiment, the media network 100 is the Internet. The Internet is a worldwide system of interconnected networks that runs the Internet Protocol (IP) to transfer data (e.g., packets). In other embodiments, the media network 100 can be other types of networks such as, for example, a token ring network, a local area network (LAN), a wide area network (WAN), or a MPEG-2 compatible broadcast network. The media network 100 can also be implemented in a wired or wireless environment.

[0029] For the first aspect of the present invention, the author module 110 provides the media server 120 with an original uncorrupt content frame. For the second aspect of the present invention, the author module 110 provides the media server 120 with a corrupt content frame. The content can be multimedia content including audio, video and data. In one embodiment, the author module 110 also provides the media server 120 with first and second identifiers. In alternate embodiments, the author module 110 can be programmed to provide a varying number of different identifiers. The identifiers can be watermarks. A watermark is a very small modification to the content frame that is not noticeable by the user. For example, a twenty byte watermark can be inserted into a four thousand byte image frame. The watermarks can be audio, video or data watermarks.

[0030] The author module 110 provides the content and watermarks in an encrypted format. The author module 110 also provides the keys to decrypt the content and watermarks. The author module 110 may be a server executing on a general purpose computer. The author module 110 can be compatible with the Moving Picture Experts Group 4 (MPEG-4) standard.

[0031] The media server 120 can be a multimedia server. The media server 120 receives the encrypted content and watermarks streams from the author module 110. The media server 120 can multicast the content to various



clients. For every client, the media server 120 selects either the first or second watermark to associate with every content frame of the content. The media server 120 can randomly select the watermark by using a random number generator. For example, the first watermark can be selected if the random number generator generates an even number and the second watermark can be selected if the random number generator generates an odd number, or vice versa. The series of watermarks thus generated is unique for every client.

[0032] The media server 120 thus serves as a toggle switch between the first and second watermarks. In one embodiment, the media server 120 transmits every content frame and the corresponding selected watermark to the client 130. In an alternate embodiment, the media server 120 transmits selected content frames and corresponding selected watermarks to the client 130. In one embodiment, the media server 120 is an Internet server. In alternate embodiments, the media server can be a LAN, WAN, or a MPEG-2 compatible broadcast network.

[0033] The client machine 130 receives the content frame and the corresponding selected watermark from the media server 130. The client machine 130 decrypts the content and the selected watermark. For the first aspect of the present invention, the client machine 130 inserts the selected watermark into the original, uncorrupt content frame. For the second aspect of the present invention, the client machine 130 inserts the selected watermark delta into the corrupt content.

[0034] The client machine 130 can be a set top box (STB), personal computer, workstation, laptop computer, or other like computing device. The client machine 130 can also be an electronic portable device such as, for example, a personal data assistant (PDA), wireless telephone, or other like devices, which can communicate with the media server 120 over a wired or wireless medium. The client machine 130 can include applications to view and display the content received from the media server 120. For example, the client machine 130 can include applications such as, for example,

QuickTime™ to play back video data. The client machine 130 can be compatible with the Moving Pictures Expert Group 4 (MPEG-4) standard.

[0035] As stated previously, for the author module 110 and the client machine 130 that are MPEG-4 standard compatible, the content can be streamed through the base layer and the first and second watermarks can be streamed through the first and second enhancement layers, respectively.

[0036] Figure 2 illustrates one embodiment of the author module 110. The author module 110 is shown including the content storage module 210, the first identifier generation module 220, the second identifier generation module 230, and the delta modules 225 and 235. The author module 110 also includes the encryption modules 240, 260 and 280, the key management modules 250, 270 and 290, and the compression module 275. The content storage module 210 is coupled to the encryption module 240 and the delta modules 225 and 235. The first and second identifier generation modules 220 and 230 are coupled to the delta modules 225 and 235, respectively. The delta modules 225 and 235 are coupled to the encryption modules 260 and 280, respectively. The delta modules 225 and 235 are also coupled to the compression module 275. The key management modules 250, 270 and 290 are coupled to the encryption modules 240, 260 and 280, respectively. Each of these modules can be a separate processing device or hardware and/or software modules operating within the media network 100 to process instructions or code for performing the operations described herein.

[0037] The content storage module 210 includes the content to be multicast across the media network 100. The content can be audio, video, data, or a combination of them. The content storage module 210 can be a storage device such as, for example, a hard disk, compact disk (CD), digital video disk (DVD), random access memory (RAM), dynamic random access memory (DRAM), or other like memory devices to store content for distribution.

[0038] The first and second identifier generation modules 220 and 230 generate the first and second watermarks respectively. The watermarks size is small as compared to the content frame size. For example, the video

content frame may include four thousand bytes of information and the watermarks may include twenty bytes of information. The delta module 225 watermarks the content stored in the content storage 210 with the first watermark and computes the delta between the watermarked content and the original content for every frame. The computed delta is referred to as the first watermark delta. Similarly, the delta module 235 watermarks the content stored in the content storage module 210 with the second watermark and computes the delta between the watermarked content and the original content for every frame. The computed delta is referred to as the second watermark delta. The run length encode module 275 performs compression, for example, run length encoding on the first and second watermark deltas.

[0039] The encryption modules 240, 260 and 280 encrypt the content frames and the first and second watermark deltas, respectively. The encryption modules 240, 260 and 280 use the keys provided by the key management modules 250, 270, and 290, respectively. The keys are transmitted to the client machine 130 in a predetermined manner. The client machine 130 uses the keys to decrypt the content frames and the first and second watermark deltas. The key management modules 240, 260 and 290 can include one or more storage devices to store a number of keys to encrypt the content frames and the first and second watermarks, respectively. The author module streams the encrypted content, deltas, and keys to the media server 120.

[0040] Figure 3 illustrates an alternate embodiment of the author module 110. The author module 110 has all the components of the author module 110 of Figure 2 and three additional components including the noise removal module 315 and the noise addition modules 385 and 395. The noise removal module 315 interfaces to the content storage module 210 and the encryption module 240. The noise addition module 385 interfaces to the delta module 225 and the encryption module 260. The noise addition module 395 interfaces to the delta module 235 and the encryption module 280. The noise removal module 315 is coupled to the noise addition modules 385 and 395. Each of

these modules can be a separate processing device or hardware and/or software modules operating within the media network 100 to process instructions or code for performing the operations described herein.

[0041] The noise removal module 315 removes a noise signal from the original content frames stored in the content storage module 210. The noise signal can be a low bandwidth or a low frequency noise signal. The resultant content frames are referred to as the corrupted content frames. The noise removal module 315 selects the noise signal such that it is a very good candidate for run length encoding and thus can be highly compressed during transmission. Also, the noise removal module 315 selects the noise signal such that the commercial value of the corrupted content is effectively destroyed.

[0042] The noise addition module 385 adds the noise signal to the first watermark delta. The noise addition module 395 adds the noise signal to the second watermark delta. The resultant signals following the noise addition modules 385 and 395 operations are also referred to as the first and second watermark deltas, respectively.

[0043] The encryption modules 240, 260 and 280 encrypt the corrupt content frames and the first and second watermark deltas, respectively. The author module 110 streams the encrypted content, deltas and keys to the media server 120.

[0044] Figure 4 illustrates an exemplary embodiment of the media server 120. The media server 120 is shown including the content receiver module 440, first and second watermark delta receiver modules 460 and 480, switch module 410, and key receiver modules 450, 470 and 490. The first and second watermark delta receiver modules 460 and 480 and the key receiver modules 470 and 490 are coupled to the switch module 410. Each of these modules can be a separate processing device or hardware and/or software modules operating within the media network 100 to process instructions or code for performing the operations described herein.

[0045] The content receiver 440 receives the content frames from the author module 110. The first and second watermark delta receiver modules 460 and 480 receive the first and second watermark deltas, respectively, from the author module 110. The key receiver modules 450, 470 and 490 receive the decryption keys for the content frames and the first and second watermark deltas, respectively, from the author module 110.

[0046] The switch module 410 includes the random number generator to select either the first or second watermark delta to associate with every content frame. The random number generator can randomly generate either 0 or 1. 0 can correspond to the first watermark and 1 can correspond to the second watermark, or vice versa. The switch module 410 thus acts as a toggle switch between the first and second watermark deltas and selects a sequence of watermark deltas. The switch module 410 selects the sequence in a manner that is unique to the particular client to whom the content is broadcast. The switch module 410 can be implemented in hardware, software, or firmware. The media server 120 streams the content, selected deltas and corresponding keys to the client machine 130.

[0047] Figure 5 illustrated an exemplary embodiment of the client machine 130. The client machine 130 is shown including the content receiver module 540, selected watermark delta receiver module 560, key management modules 550 and 570, decryption modules 520 and 530, the decompression module 575 and the combine module 580. The content receiver module 540 and the key management module 550 are coupled to the decryption module 520. The selected watermark delta receiver module 560 and the key management module 570 are coupled to the decryption module 530. The decryption module 520 is coupled to the combine module 580. The decompression module 575 interfaces to the decryption module 530 and the combine module 580. Each of these modules can be a separate processing device or hardware and/or software modules operating within the media network 100 to process instructions or code for performing the operations described herein.

[0048] The content receiver module 540 receives the content frames from the media server 120. The selected watermark delta receiver module receives the watermark deltas selected by the switch module 410 of the media server 120. The key management modules 550 and 570 receive the decryption keys for the content frames and the selected watermark deltas, respectively, from the media server 120. The decryption modules 520 and 530 use the keys provided by the key management modules 520 and 530 to decrypt the content frames and the selected watermark delta, respectively.

[0049] For the first aspect of the present invention, the content frames include the original uncorrupt content frames. For the second aspect of the present invention, the content frames includes the corrupt content frames and the selected watermark deltas include the low bandwidth noise signal added to the watermark deltas.

[0050] The decompression module 575 performs decompression, for example, run length decoding, on the selected watermark deltas. The combine module 580 inserts the selected watermark deltas into the content frames. The combine module operation can include an exclusive or (XOR) logic operation between the content frames and the selected watermark deltas. The XOR logic operation can be performed for audio, video or data frames and deltas.

[0051] Figure 6 illustrates exemplary embodiments of the data streams to perform client side fingerprinting (or watermarking) for multicast data. Three data streams 610, 620 and 630 are shown. In one embodiment, the content data stream 610 includes the four content frames 650, 652, 654 and 656. In other embodiments, different numbers of content frames 650-656 are possible. The first watermark delta stream 620 includes the four first watermark delta packets 660, 662, 664 and 666. Every first watermark delta packet 660-666 includes the same first watermark delta. The second watermark delta stream 630 includes the four second-watermark delta packets 670, 672, 674 and 676. Every second watermark delta packet 670-676 includes the same second watermark delta.

[0052] Every content frame 650-656 is associated with the first and second watermark delta packets shown directly above it. For example, the content frame 650 is associated with the first watermark delta packet 660 and the second watermark delta packet 670. The switch module 410 can select either the first watermark delta packet 660 or the second watermark delta packet 670 to be associated with the content frame 650. If the switch module 410 selects the first watermark delta packet 660, for example, the client machine 130 inserts the watermark included in the first watermark delta packet 660 into the content frame 650.

[0053] The switch module 410 generates a sequence of the watermark delta packets by associating every content frame 650-656 with either the first watermark delta packet 660-666 or the second watermark delta packet 670-676. The switch module 410 can generate a unique sequence for every client to whom the content stream is broadcast. The following example illustrates the point. Suppose the media server 130 is requested to multicast the content stream 610 to Tom, Bill and John. The switch module 410 can generate a sequence for Tom including the first, second, first and second watermark delta packets. The switch module 410 can generate a sequence for Bill including the second, first, second and first watermark delta packets. Finally, the switch module 410 can generate a sequence for John including the second, second, first and second watermark delta packets. The sequences uniquely identify the recipients of the content stream 610 as Tom, Bill or John.

[0054] The content frame stream 610 can be placed in the MPEG-4 standard compatible base layer. The first watermark delta stream 620 can be placed in the MPEG-4 standard compatible enhancement layer one. The second watermark delta stream 630 can be placed in the MPEG-4 standard compatible enhancement layer two.

[0055] Figure 7 illustrates one embodiment of a method to perform on the fly fingerprinting for media content. At block 710, the first and second watermark deltas are computed. The first watermark delta represents the delta between the original uncorrupt content frame and the original

uncorrupt content frame watermarked with the first watermark. The second watermark delta represents the delta between the original uncorrupt content frame and the original uncorrupt content frame watermarked with the second watermark.

[0056] At block 715, the first and second watermark deltas are compressed. At block 720, the first and second watermark deltas and the original uncorrupt content frame is encrypted. At block 730, either the first or second watermark delta is selected to be associated with the original uncorrupt content frame. This process of block 730 is repeated for every original uncorrupt content frame in a manner that generates a unique sequence of watermark deltas for a particular client. The operations of the blocks 710, 715, 720 and 730 are performed on the server side by the author and server modules.

[0057] At block 740, the watermark delta selected at block 730 and original uncorrupt content frame are transmitted to the client machine 130 as two different data streams. At block 750, the client machine 130 decrypts the selected watermark delta and the original uncorrupt content frame. At block 755, the client machine 130 decompresses the selected watermark delta. At block 760, the client machine inserts the selected watermark delta into the original uncorrupt content frame. The process at block 760 can be performed through an exclusive OR (XOR) operation.

[0058] Figures 8A and 8B illustrate an alternate embodiment of the method to perform on the fly fingerprinting for media content. The method is illustrated by the way of an example for the original content frame data shown in block 810. The low bandwidth noise signal shown in block 815 is removed from the original content frame data shown in block 810. The corrupt content frame data that results is shown in block 820. A first watermark is inserted into the original content frame data shown in block 810. The resultant data is shown in block 825. The delta between the data shown in block 825 and the data shown in block 810 is computed. This delta is referred to as the first watermark delta and is shown in block 830. The low



bandwidth noise signal shown in block 815 is added to the first watermark delta. The resultant data is also referred to as the first watermark delta and is shown in block 835. The first watermark delta shown in block 835 is compressed. The result is shown in block 840.

[0059] The processes performed with respect to the first watermark are also performed with respect to a second watermark such that a run length encoded second watermark delta is generated (not shown).

[0060] Either the first or the second watermark delta is associated with every corrupt content frame of the content. A sequence of watermark deltas is thus generated. The sequence is generated in a manner that is unique for a particular client. An exemplary sequence is shown in block 845 where 1 can represent the first watermark delta and 0 can represent the second watermark delta. The selected watermark delta and the corrupt content frame data shown in block 820 is transmitted to the client machine. The client machine decompresses the selected watermark delta. If the selected watermark delta, for example, is the first watermark delta, block 850 shows the decompressed first watermark delta. The client machine inserts the selected watermark delta into the corrupt content shown in block 820. If the selected watermark delta is the first watermark delta, the resultant data includes the original content shown in block 810 and the first watermark delta shown in block 830. The resultant data is shown in block 855.

[0061] Figure 9 illustrates a computer in block diagram form, which may be representative of any author module, media server or client machine. The block diagram is a high level conceptual representation and may be implemented in a variety of ways and by various architectures. The bus system 902 interconnects a Central Processing Unit (CPU) 904, a ROM 906, a RAM 908, storage 910, a display 920, an audio 922, a keyboard 924, a pointer 926, miscellaneous input/output (I/O) devices 928, and communications 930. The bus system 902 may be for example, one or more of such buses as a system bus, a Peripheral Component Interconnect (PCI), an Advanced Graphics Port (AGP), a Small Computer System Interface (SCSI), and an

Institute of Electrical and Electronics Engineers (IEEE) standard number 1394 (Fire Wire). The CPU 904 may be a single, multiple, or even a distributed computing resource. The ROM 906 may be any type of non-volatile memory that may be programmable such as mask programmable and flash. The RAM 908 may be, for example, static, dynamic, synchronous, asynchronous, or any combination. The storage 910 may be a Compact Disc (CD), a Digital Versatile Disk (DVD), a hard disk, an optical disk, a tape, a flash, a memory stick or a video recorder. The display 920 might be, for example, a Cathode Ray Tube (CRT), a Liquid Crystal Display (LCD), a projection system or a Television (TV). The audio 922 may be a monophonic, a stereo, or a three dimensional sound card. The keyboard 924 may be a keyboard, a musical keyboard, a keypad, or a series of switches. The pointer 926 may be, for example, a mouse, a touch pad, a trackball, or a joystick. The I/O device 928 might be a voice command input device, a thumbprint input device, a smart card slot, a Personal Computer Card (PC Card) interface, or a virtual reality accessory. The I/O device 928 can be connected via an input/output port 929 to other devices or systems. An example of a miscellaneous I/O device 928 would be a Musical Instrument Digital Interface (MIDI) card with the I/O port 929 connected to the musical instrument(s). The communications device 930 might be, for example, an Ethernet adapter for a local area network (LAN) connection, a satellite connection, a set-top box adapter, a Digital Subscriber Line (xDSL) adapter, a wireless modem, a conventional telephone modem, a direct telephone connection, a Hybrid-Fiber Coax (HFC) connection, or a cable modem. The external connection port 932 may provide for any interconnection, as needed, between a remote device and the bus system 902 through the communications device 330. For example, the communications device 930 might be an IEEE 802.3 (Ethernet) adapter that is connected via the connection port 932 to, for example, an external DSL modem. It is appreciated that depending on the actual implementation of a computer system, the computer system may include some, all, more, or a rearrangement

of components in the block diagram. For example, a thin client might consist of a wireless hand held device that lacks, for example, a traditional keyboard.

[0062] These and other embodiments of the present invention may be realized in accordance with these teachings and it should be evident that various modifications and changes may be made in these teachings without departing from the broader spirit and scope of the invention. The specification and drawings are, accordingly, to be regarded in an illustrative rather than restrictive sense and the invention measured only in terms of the claims.

[0063] In addition, the methods as described above can be stored in memory of a computer system as a set of instructions to be executed. In addition, the instructions to perform the methods as described above could alternatively be stored on other forms of computer-readable mediums, including magnetic and optical disks. For example, the method of the present invention can be stored on computer-readable mediums, such as magnetic disks or optical disks that are accessible via a disk drive (or computer-readable medium drive).

CLAIMS

What is claimed is:

1. A computer-implemented method to fingerprint content comprising a plurality of content frames, the method including:
  - generating a sequence of identifiers by associating either a first or a second identifier with each content frame of at least a portion of the plurality of content frames;
  - transmitting the plurality of content frames and the sequence of identifiers to a client; and
  - inserting each associated identifier of the sequence of identifiers into the each content frame of the at least a portion of the plurality of content frames;
  - wherein the sequence of identifiers is generated in a manner that it is unique for the client.
2. The computer-implemented method of claim 1, including utilizing any one of an audio, video and data as the content.
3. The computer-implemented method of claim 1, including using watermarks as the first and second identifiers.
4. The computer-implemented method of claim 1, including generating the sequence of identifiers using a server.
5. The computer-implemented method of claim 1, including transmitting the sequence of identifiers and the plurality of content frames as three different data streams.
6. The computer-implemented method of claim 1, including using moving pictures expert group (MPEG) standard 4 compatible enhancement layers to transmit the sequence of identifiers and using a MPEG standard 4 compatible base layer to transmit the plurality of content frames.

7. The computer-implemented method of claim 1, including using moving pictures expert group (MPEG) standard 2 compatible intellectual property management and protection (IPMP) streams to transmit the sequence of identifiers and the plurality of content frames.
8. The computer-implemented method of claim 1 including inserting the identifier into the content frame using an exclusive OR (XOR) operation.
9. The computer-implemented method of claim 1, including randomly generating the sequence of identifiers.
10. A machine readable medium providing instructions, which if executed by a processor, causes the processor to perform a method to fingerprint content comprising a plurality of content frames, the method including:
  - generating a sequence of identifiers by associating either a first or a second identifier with each content frame of at least a portion of the plurality of content frames;
  - transmitting the plurality of content frames and the sequence of identifiers to a client; and
  - inserting each associated identifier of the sequence of identifiers into the each content frame of the at least a portion of the plurality of content frames;
  - wherein the sequence of identifiers is generated in a manner that it is unique for the client.
11. The machine readable medium of claim 10, including utilizing any one of an audio, video and data as the content.
12. The machine readable medium of claim 10, including using watermarks as the first and second identifiers.
13. The machine readable medium of claim 10, including generating the sequence of identifiers using a server.

14. The machine readable medium of claim 10, including transmitting the sequence of identifiers and the plurality of content frames as three different data streams.

15. The machine readable medium of claim 10, including using moving pictures expert group (MPEG) standard 4 compatible enhancement layers to transmit the sequence of identifiers and using a MPEG standard 4 compatible base layer to transmit the plurality of content frames.

16. The machine readable medium of claim 10, including using moving pictures expert group (MPEG) standard compatible intellectual property management and protection (IPMP) streams to transmit the sequence of identifiers and the plurality of content frames.

17. The machine readable medium of claim 10, including inserting the identifier into the content frame using an exclusive OR (XOR) operation.

18. The machine readable medium of claim 10, including randomly generating the sequence of identifiers.

19. A computing system to fingerprint content comprising a plurality of content frames comprising:

a server to generate a sequence of identifiers by associating either a first or a second identifier with each content frame of at least a portion of the plurality of content frames, and to transmit the plurality of content frames and the sequence of identifiers to a client; and

the client to insert each associated identifier of the sequence of identifiers into the each content frame of the at least a portion of the plurality of content frames;

wherein the server is to generate the sequence in a manner that is unique for the client.

20. The computing system of claim 19, wherein the content includes multicast content.

21. The computing system of claim 19, wherein the content comprises any one of the group including audio, video and data content.
22. The computing system of claim 19, wherein the first and second identifiers are watermarks.
23. The computing system of claim 19, wherein the server includes a toggle switch to select between the first and second identifiers to generate the sequence of identifiers.
24. The computing system of claim 19, wherein the sequence of identifiers and the plurality of content frames are transmitted as three different data streams.
25. The computing system of claim 19, wherein the sequence of identifiers are transmitted through moving pictures expert group (MPEG) standard 4 compatible enhancement layers and the plurality of content frames are transmitted through a MPEG standard 4 compatible base layer.
26. The computing system of claim 19, wherein the sequence of identifiers and the plurality of content frames are transmitted through moving pictures expert group (MPEG) standard compatible intellectual property management and protection (IPMP) streams.
27. The computing system of claim 19, wherein an author module generates the first and second identifiers.
28. The computing system of claim 19, wherein an exclusive OR (XOR) module inserts the identifier into the content frame.
29. The computing system of claim 19, wherein the server randomly generates the sequence of identifiers.
30. A computing system to fingerprint content comprising a plurality of content frames comprising:

means for generating a sequence of identifiers by associating either a first or a second identifier with each content frame of at least a portion of the plurality of content frames, and for transmitting the plurality of content frames and the sequence of identifiers to a client; and

means for inserting each associated identifier of the sequence of identifiers into the each content frame of the at least a portion of the plurality of content frames;

wherein the means for generating the sequence generate the sequence in a manner that is unique for the client.

31. A network comprising:

an author module;

a server;

a client;

the author module to create first and second identifiers;

the server to generate a sequence of identifiers by associating either the first or the second identifier with each content frame of at least a portion of a plurality of content frames, and

to transmit the sequence of identifiers and the plurality of content frames to a client; and

the client configured to insert each associated identifier of the sequence of identifiers into the each content frame of the at least a portion of the plurality of content frames;

wherein the server is configured to generate the sequence in a manner that it is unique for the client.

32. A computer-implemented method to fingerprint a content frame comprising:

corrupting the content frame by removing a noise signal from the content frame;

computing a watermark delta by adding an identifier to the noise signal;



transmitting the corrupt content frame and the watermark delta to a client; and

inserting the watermark delta into the corrupt content frame using the client.

33. The computer-implemented method of claim 32, including utilizing any one of an audio, a video and a data content frame as the content frame.

34. The computer-implemented method of claim 32, including using a watermark as the identifier.

35. The computer-implemented method of claim 32, including using a low bandwidth random noise signal as the noise signal.

36. The computer-implemented method of claim 32, including removing the noise signal to render the content frame non-viewable.

37. The computer-implemented method of claim 32, including removing the noise signal to reduce a size of the content frame.

38. The computer-implemented method of claim 32, including run length encoding the watermark delta prior to transmission thereof to the client.

39. The computer-implemented method of claim 32, including using a moving pictures expert group (MPEG) standard 4 compatible enhancement layer to transmit the watermark delta and using a MPEG standard 4 compatible base layer to transmit the content frame.

40. The computer-implemented method of claim 32, including using moving pictures expert group (MPEG) standard compatible intellectual property management and protection (IPMP) streams to transmit the watermark delta and the content frame.

41. A machine-readable medium providing instructions, which if executed by a processor, causes the processor to perform a method to fingerprint a content frame comprising:

corrupting the content frame by removing a noise signal from the content frame;

computing a watermark delta by adding an identifier to the noise signal;

transmitting the corrupt content frame and the watermark delta to a client; and

inserting the watermark delta into the corrupt content frame using the client.

42. The machine readable medium of claim 41, including utilizing any one of an audio, a video and a data content frame as the content frame.

43. The machine readable medium of claim 41, including using a watermark as the identifier.

44. The machine readable medium of claim 41, including using a low bandwidth random noise signal as the noise signal.

45. The machine readable medium of claim 41, including removing the noise signal to render the content frame unviewable.

46. The machine readable medium of claim 41, including removing the noise signal to reduce a size of the content frame.

47. The machine readable medium of claim 41, including run length encoding the first and second watermark deltas prior to transmission thereof to the client.

48. The machine readable medium of claim 41, including using a moving pictures expert group (MPEG) standard 4 compatible enhancement layer to transmit the watermark delta and using a MPEG standard 4 compatible base layer to transmit the content frame.

49. The machine readable medium of claim 41, including using moving pictures expert group (MPEG) standard compatible intellectual property management and protection (IPMP) streams to transmit the watermark delta and the content frame.
50. A computing system to fingerprint a content frame comprising:  
an author module to corrupt the content frame by removing a noise signal from the content frame;  
a delta module to compute a watermark delta by adding an identifier to the noise signal;  
a server to transmit the corrupt content frame and the watermark delta to a client; and  
the client to insert the watermark delta into the associated corrupt content frame.
51. The computing system of claim 50, wherein the content frame includes a multicast content frame.
52. The computing system of claim 50, wherein the author module creates the identifier.
53. The computing system of claim 50, wherein the content frame comprises one of a group including audio, video and data content frames.
54. The computing system of claim 50, wherein the identifier includes a watermark.
55. The computing system of claim 50, wherein the noise signal includes a low bandwidth random noise signal.
56. The computing system of claim 50, wherein the noise signal is removed to render the content frame unviewable.
57. The computing system of claim 50, wherein the noise signal is removed to reduce a size of the content frame.

58. The computing system of claim 50, wherein the watermark delta is run length encoded prior to transmission thereof to the client.

59. The computing system of claim 50, wherein a moving pictures expert group (MPEG) standard 4 compatible enhancement layer is used to transmit the watermark delta and MPEG standard 4 compatible base layer is used to transmit the content frame.

60. The computing system of claim 50, wherein moving pictures expert group (MPEG) standard compatible intellectual property management and protection (IPMP) streams are used to transmit the watermark delta and the content frame.

61. A computing system to fingerprint a content frame comprising:  
means for creating an identifier;  
means for corrupting the content frame by removing a noise signal from the content frame;  
means for computing a watermark delta by adding the identifier to the noise signal;  
means for transmitting the corrupt content frame and the watermark delta to a client; and  
means for inserting the watermark delta into the corrupt content frame by using the client.

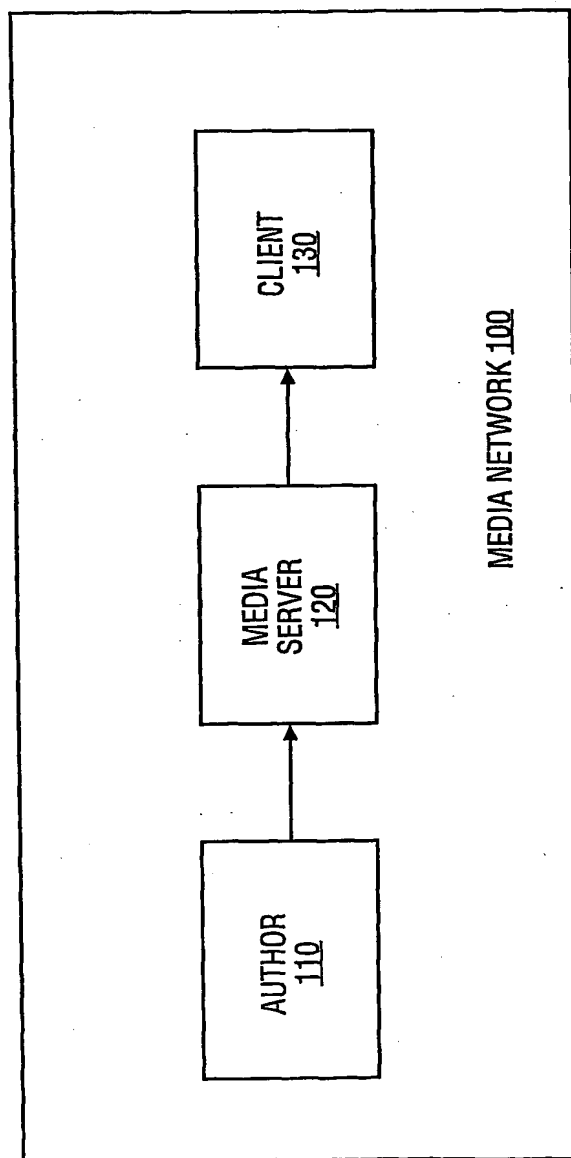


FIG. 1

2/10

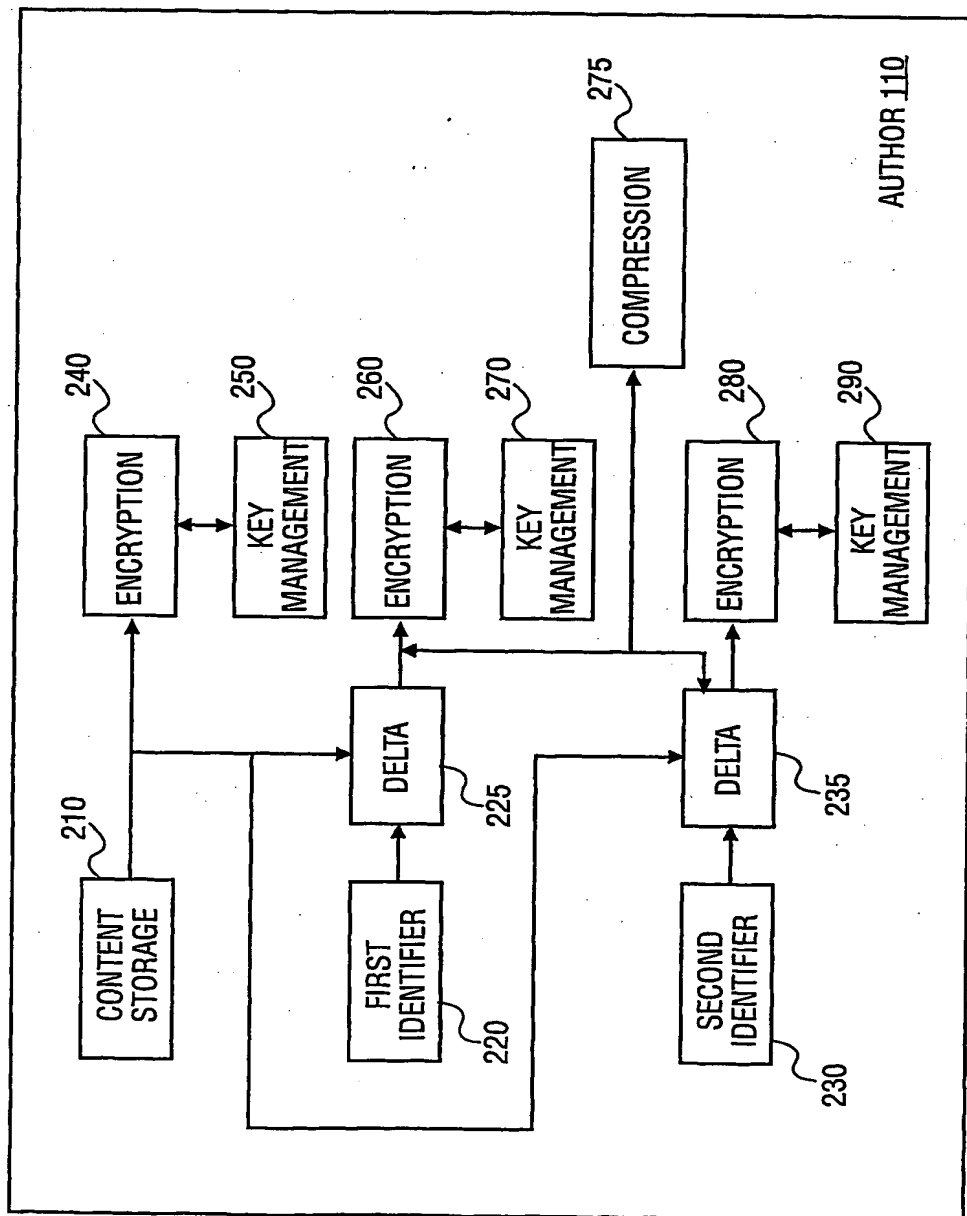


FIG. 2

FIG. 3

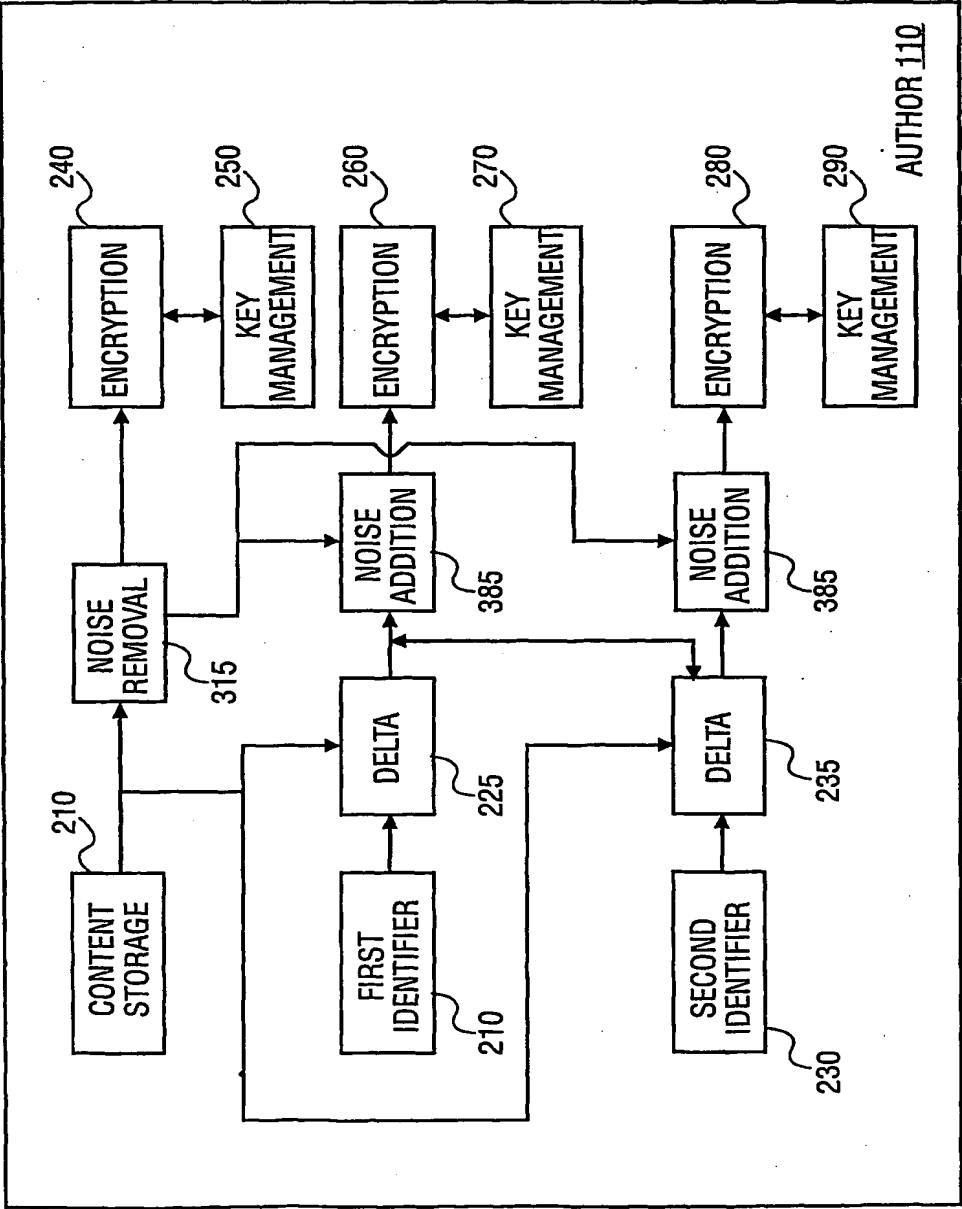


FIG. 4

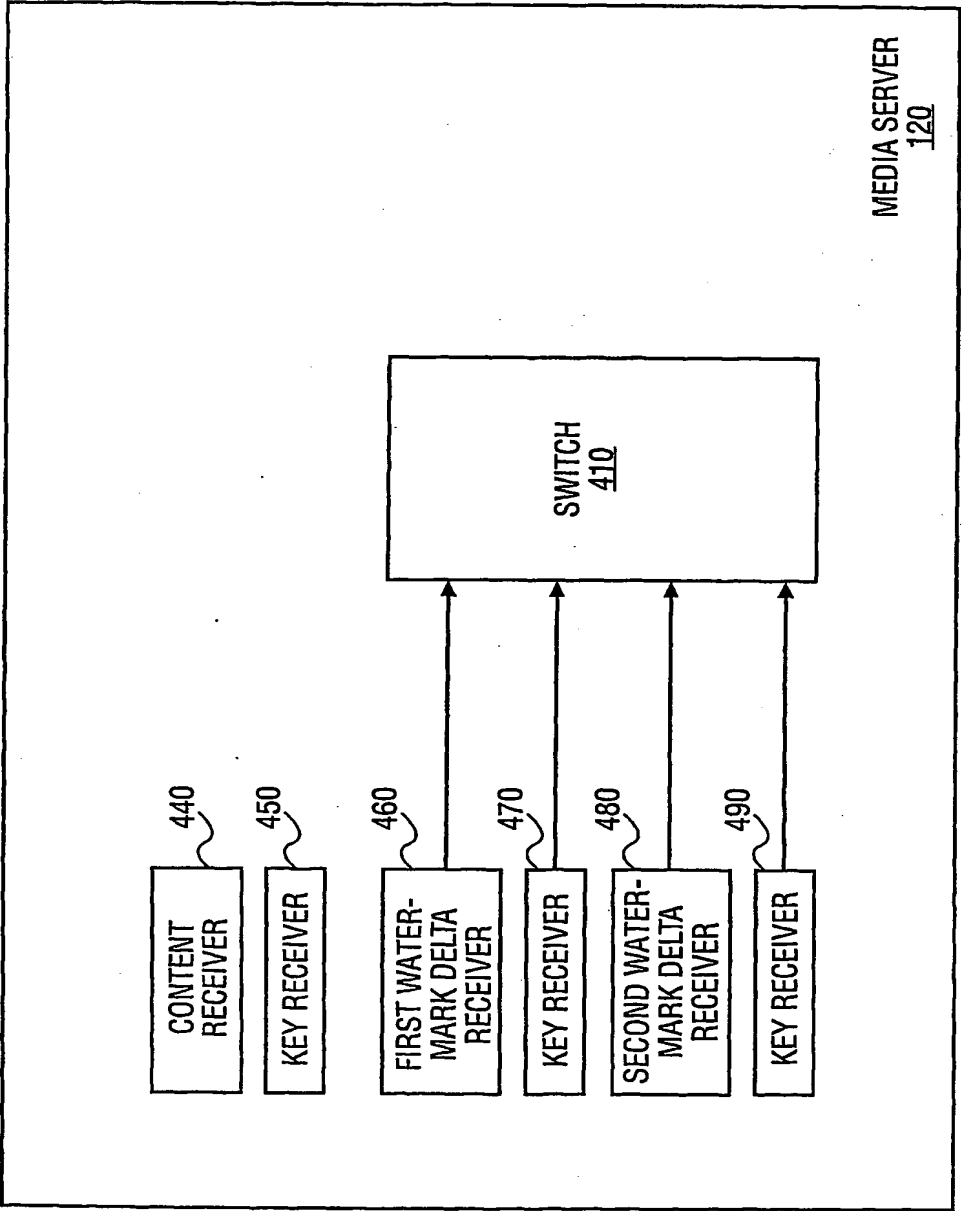
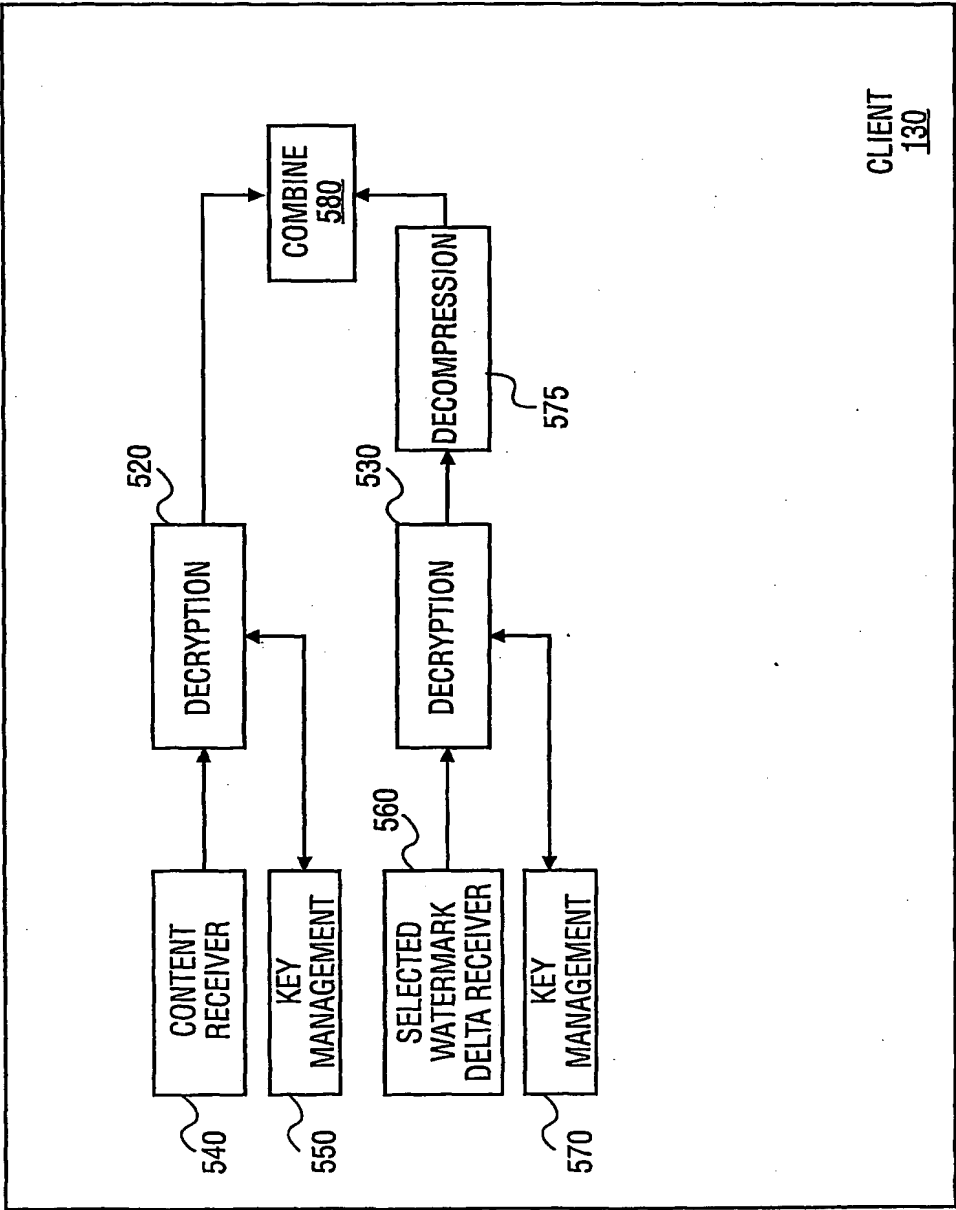




FIG. 5



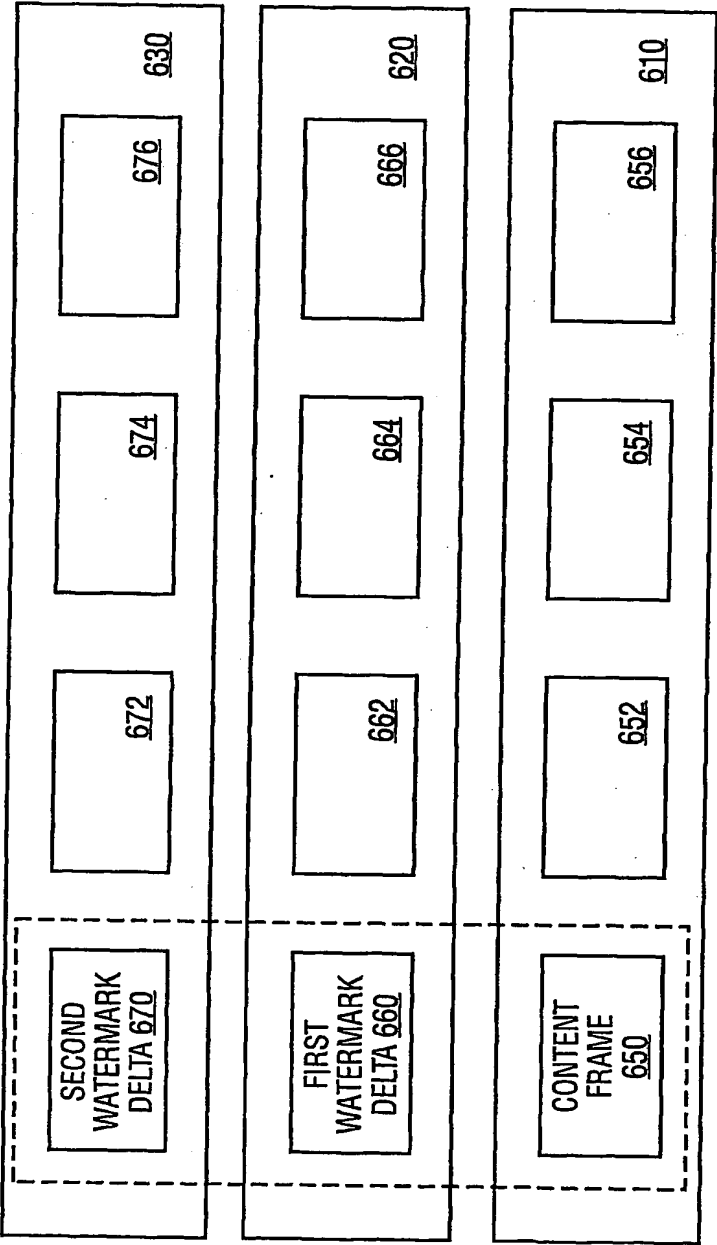


FIG. 6

7/10

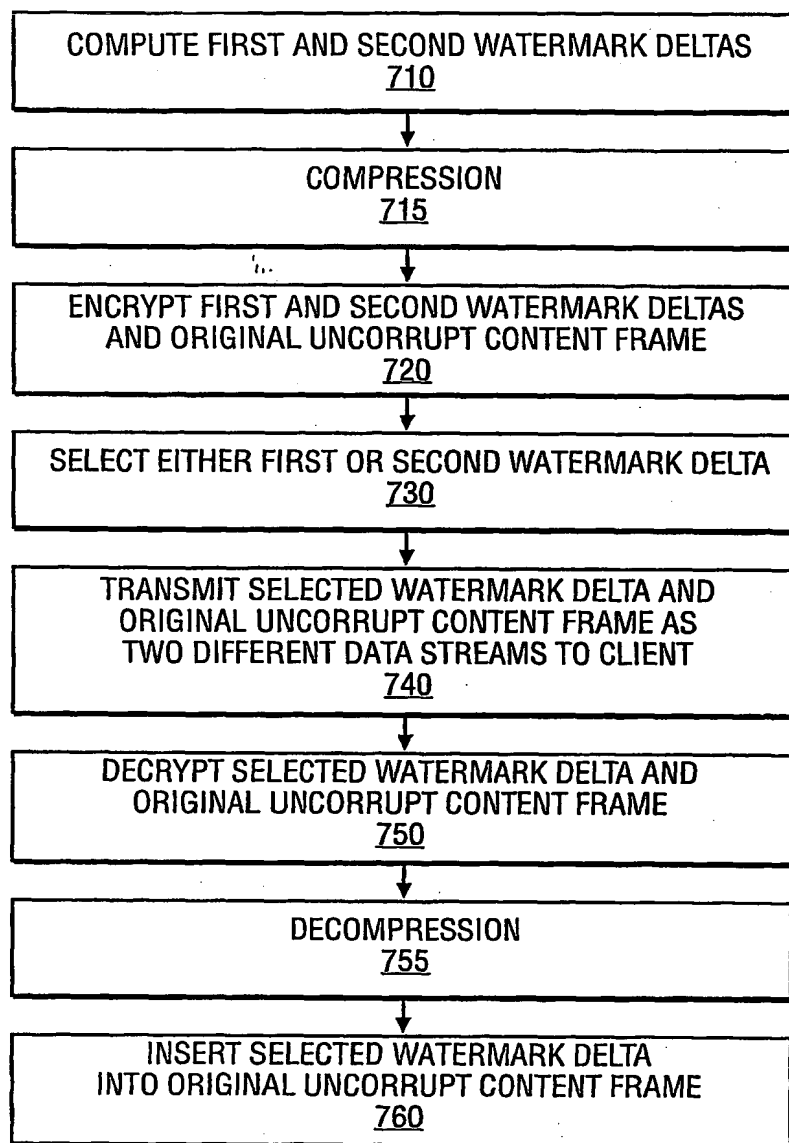


FIG. 7

8/10

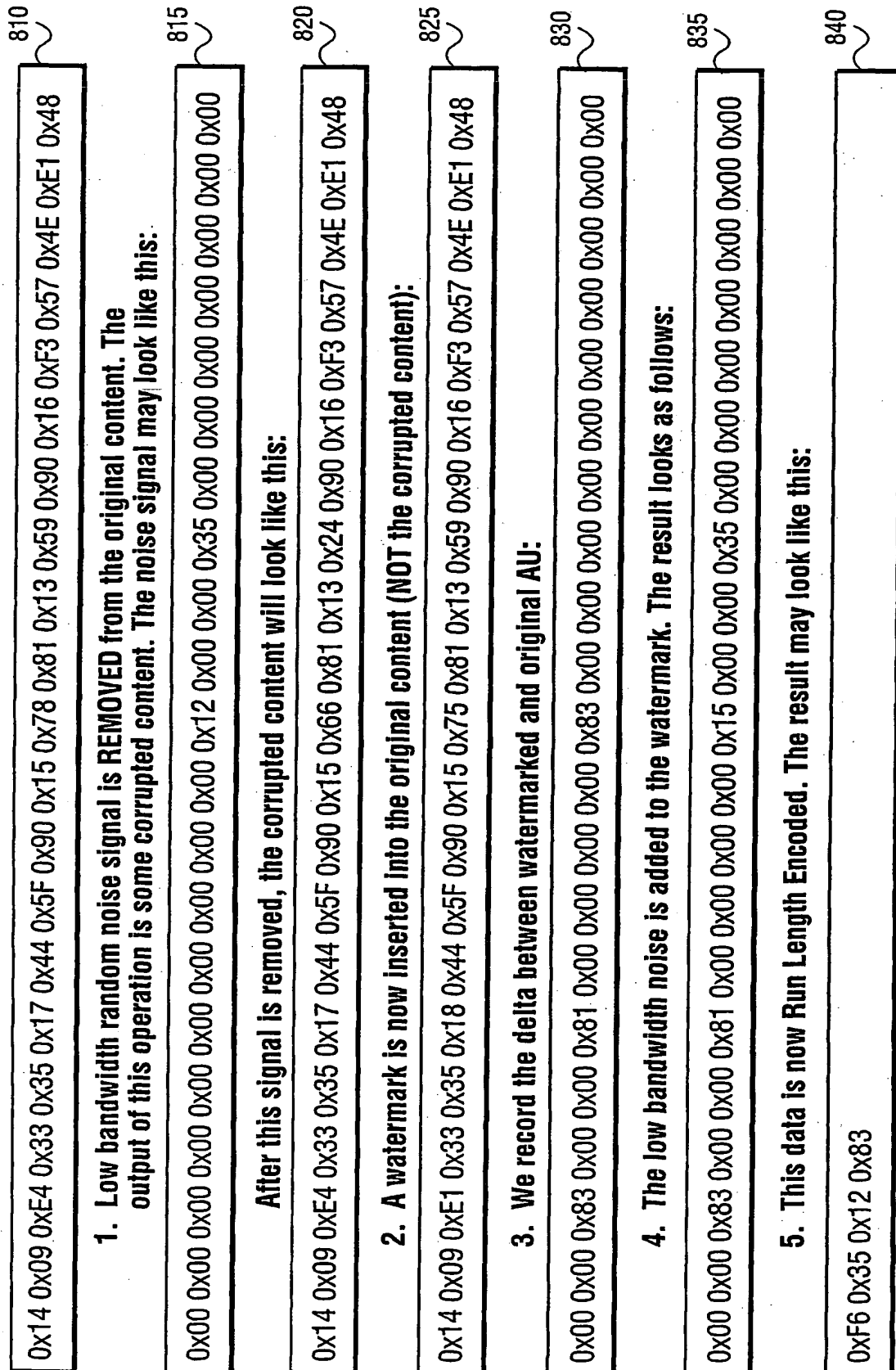


FIG. 8A

9/10

6. The Sentriq Agent generates a Unique Random Sequence for each client. This sequence could look like this:

111010010 845

7. Based on this random sequence, the appropriate watermark data (+ random noise) is selected by the agent

8. The watermark data (+ noise) is sent to the client terminal.

9. The Watermark (+ noise) is Run Length Decoded. For our example content, watermark 1 will look like this:

0x00 0x00 0x83 0x00 0x00 0x81 0x00 0x00 0x00 0x15 0x00 0x00 0x35 0x00 0x00 0x00 0x00 0x00 0x00 850

10. This data is now added to the corrupted AU that the terminal has received from the Media server. This produces the original content + watermark. The noise is removed:

0x14 0x09 0xE1 0x33 0x35 0x18 0x44 0x5F 0x90 0x15 0x75 0x81 0x13 0x59 0x90 0x16 0xF3 0x57 0x4E 0xE1 0x48 855

The AU may now be decoded/rendered by terminal.

FIG. 8B

10/10

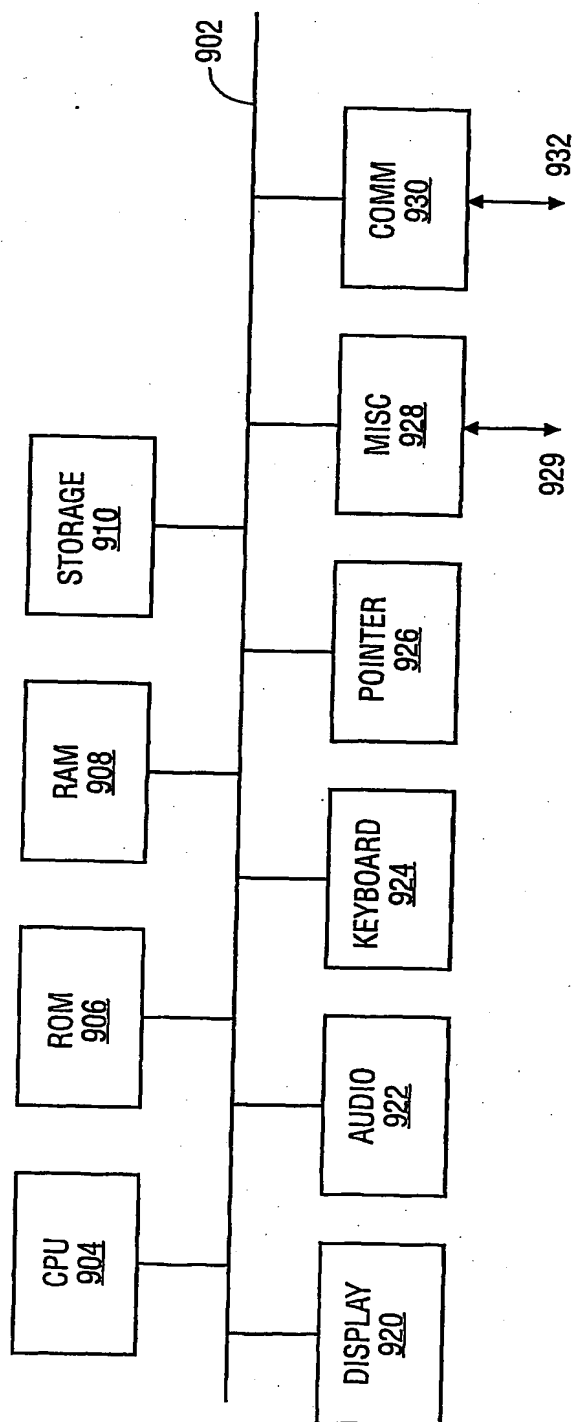


FIG. 9

## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/US01/29031

<b>A. CLASSIFICATION OF SUBJECT MATTER</b> IPC(7) : H04L 9/32, 9/18; H04K 9/18; G06K 9/64 US CL : 713/176; 380/36, 37, 252; 382/284 According to International Patent Classification (IPC) or to both national classification and IPC			International Patent Classification?: H04L 9/32, 9/18, 9/18, G06K 9/64
<b>B. FIELDS SEARCHED</b> Minimum documentation searched (classification system followed by classification symbols) U.S. : 713/163, 176, 179; 380/28, 36, 37, 46, 54, 201, 202, 210, 217, 252, 254; 382/284; 705/57, 58; 700/94 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) Please See Extra Sheet.			
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>			
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.	
X	US 6,208,745 B1 (FLORENCIO et al.) 27 March 2001 (27.03.2001), column 3, lines 14-16, 20-24, and 37-42, column 4, lines 41-53, column 5, lines 40-52 and 59-67, column 6, lines 1-10 and 20-25, figure 1, figure 2, items 204, 208, 210, 212, 216.	1,3,5,6,9,10,12, 14,15,18,30	
---		---	
Y		2,4,8,11,13,17,19 -22, 24,25,27-29, 31, 39, 48, 52, 59	
---		---	
A		7,16,23,26	
Y	US 6,209,094 B1 (LEVINE et al.) 27 March 2001 (27.03.2001), column 1, lines 33-40 and 58-61, column 2, lines 1-3, column 4, lines 66-67, column 5, lines 1-19, column 16, lines 26-30 and 50-55, column 29, lines 5-11, figure 1, figure 12, item 1206.	2, 4, 8, 11, 13, 17, 19 - 22, 24,25,27-29, 31, 51	
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.			
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed		"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family	
Date of the actual completion of the international search 01 DECEMBER 2001		Date of mailing of the international search report 27 DEC 2001	
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230		Authorized officer JUSTIN T. DABROW <i>James R. Matthews</i> Telephone No. (703) 305-3872	

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/US01/29031

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,915,027 A (COX et al.) 22 June 1999 (22.06.1999), column 1, lines 4-5, column 4, lines 54-65, column 8, lines 40-45, figure 1, items 12, 13, 14, 15, 16, 17.	32-35, 41-44, 50, 53-55, 61
—		—
A		36-38, 40, 45-47, 49, 56-58, 60
—		—
Y		39, 48, 51, 52, 59



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/US01/29031

## B. FIELDS SEARCHED

Electronic data bases consulted (Name of data base and where practicable terms used):

EAST(USPAT, EPO, JPO, DERWENT, US-PGPUB)

search terms: watermark, fingerprint, associate, correspond, reference, accordance, point, direct, identify, label, frame, block, subblock, portion, part, partition, segment, file, transmit, send, upload, uplink, broadcast, insert, input, add, combine, exclusive OR, XOR, noise, residue, remove, extract, subtract, take, eliminate